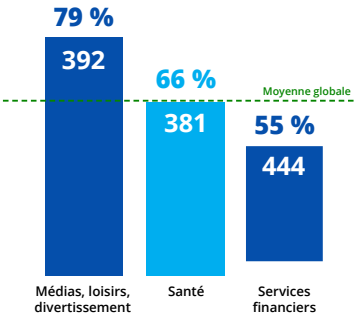
ThreatQ pour le secteur de la santé

Vu les énormes volumes de données médicales et personnelles qu'ils conservent et traitent pour leurs patients, les établissements de santé sont devenus des cibles attrayantes pour les pirates informatiques. Les dossiers médicaux électroniques contiennent des données précieuses telles que le nom complet, la date de naissance, le numéro de sécurité sociale et les informations de facturation d'un patient, et constituent dès lors une véritable mine d'or numérique pour les escrocs, attirés par les perspectives lucratives associées à la vente d'informations personnelles sur le marché noir.

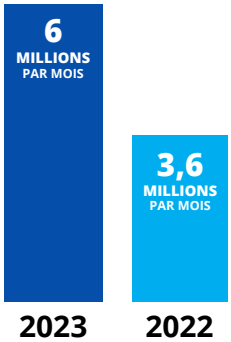
Sophos, une société de logiciels et de matériel de sécurité, a mené une enquête agnostique qui montre que 66 % des établissements de santé ont été victimes d'un ransomware l'année dernière, contre 34 % en 2020[1], soit une augmentation de 94 % en un an. Ce résultat est la preuve que les cyberadversaires ont considérablement amélioré leurs techniques d'exécution d'attaques plus dévastatrices et à plus grande échelle. Généralement, ces campagnes ont recours au vol d'identifiants et infectent plusieurs machines avant d'être détectées, compromettant ainsi le fonctionnement du système de santé. Selon un rapport du New York Times de 2020, des pirates russes ont lancé une attaque par ransomware contre United Health Services, un prestataire de soins de santé disposant d'un réseau de plus de 400 établissements. À ce stade, cette attaque était l'incident le plus important de ce type[2]. Ces attaques, et plus récemment l'activité d'un groupe prénommé Clop[3], font office d'avertissement pour les prestataires de soins de santé et mettent en évidence la nécessité impérieuse de renforcer les défenses de cybersécurité au sein des systèmes de santé du monde entier. Dans ce contexte, les établissements de santé souscrivent des cyberassurances et doivent de ce fait investir dans des défenses de cybersécurité plus robustes[4].

ATTAQUES PAR RANSOMWARE PAR SECTEUR



Source : Sophos[6]

NOMBRE DE PERSONNES VICTIMES DE CYBERATTAQUES PAR MOIS



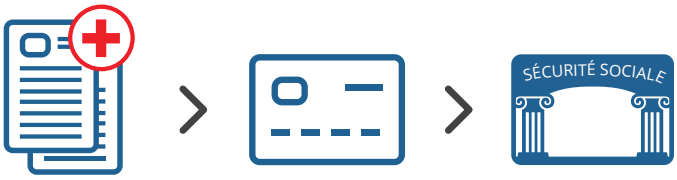
Source : Chief Healthcare Executive®[5]

PRINCIPAUX DÉFIS

DISPONIBILITÉ DES DONNÉES

Un accès instantané et fiable aux données pertinentes des patients sauve des vies, et leurs dossiers doivent pouvoir être consultés sur demande par le personnel médical. L'attention portée au bien-être des patients et aux résultats cliniques l'emporte presque toujours sur la protection des données. Ceci explique le recours constant à des processus de partage des informations non sécurisés et des technologies de communication obsolètes. Or la vigilance est impérative. En effet, les données médicales confidentielles sont particulièrement vulnérables aux attaques par malware et par ransomware, et exigent par conséquent des contrôles de sécurité rigoureux. La Threat Intelligence peut fournir des informations inestimables sur les motivations des attaquants et leurs tactiques, techniques et procédures, et qui permettent de déterminer comment renforcer le plus efficacement les défenses.

COMPARAISON SUR LE DARK WEB : N° SS = 1 $, CARTE DE CRÉDIT = 5 $, DOSSIER MÉDICAL = 1 000 $ – PRIX PAR DOSSIER[7]



Dossier médical **1 000 $**

Carte de crédit **5 $**

N° SS **1 $**

Selon The HIPAA Journal, un fournisseur de solutions de conformité à la loi HIPAA, si les dossiers médicaux intéressent tant les cybercriminels, c'est qu'ils peuvent être utilisés beaucoup plus longtemps que les cartes de crédit avant la découverte de la compromission[8].

SYSTÈMES D'ANCIENNE GÉNÉRATION

En général, les infrastructures et équipes médicales recourent à des systèmes et des appareils obsolètes, exécutant d'anciennes versions de logiciels et d'outils de sécurité qui sont extrêmement vulnérables aux compromissions. La nécessité de pouvoir accéder aux informations des patients à tout moment et en tout lieu fait que les administrateurs et les professionnels de la santé sont souvent réfractaires à une mise à niveau des appareils, synonyme d'interruptions potentielles de la prestation des soins. Toutefois, il suffit parfois d'un système archaïque, non mis à jour ou compromis pour que l'établissement soit victime d'une violation de sécurité majeure.

Pour prioriser efficacement les mesures correctives à mettre en œuvre afin de protéger leurs ressources informatiques, à la fois les anciennes et les nouvelles, les systèmes de santé doivent corréler les données de Threat Intelligence et les failles de sécurité potentielles dans leur environnement. Les prestataires disposant de ressources de sécurité limitées peuvent ainsi se concentrer sur les vulnérabilités de l'infrastructure critique qui posent le plus haut risque pour l'établissement.

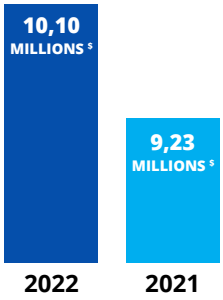
TECHNOLOGIES MODERNES

Ces technologies, telles que les applications de gestion de dossiers médicaux électroniques et les dispositifs médicaux connectés à l'Internet des objets (IoT), offrent une accessibilité, une connectivité et une évolutivité exceptionnelles, améliorant l'efficacité et les soins aux patients. Malheureusement, elles élargissent la surface d'attaque, de sorte que les données sensibles sont sans cesse exposées aux menaces conçues pour les dérober ou les exploiter à mauvais escient. Il reste difficile de trouver l'équilibre optimal entre technologies de numérisation avancées et stratégies de sécurité mises en œuvre pour protéger les ressources face à l'expansion de la surface d'attaque. Les réévaluations automatiques des menaces, scoring, niveaux de risque et priorités en fonction des données de Threat Intelligence les plus récentes et de l'évolution de l'environnement interne permettent toutefois de rester concentré sur les stratégies de réduction des risques les plus judicieuses.

OPÉRATIONS DE SÉCURITÉ DE POINTE ORIENTÉES SUR LES DONNÉES

Une plate-forme d'opérations de sécurité robuste fournit aux prestataires de soins de santé le contexte, la personnalisation et la priorisation dont ils ont besoin. Ils peuvent ainsi prendre des décisions plus avisées, accélérer la détection et la réponse à incidents, et favoriser la collaboration entre équipes. La plate-forme ThreatQ, qui sert de centre d'opérations de renseignement pour de nombreux secteurs, assemble et corrèle les données structurées et non structurées issues d'une multitude de sources, internes comme externes.

COÛT MOYEN D'UNE COMPROMISSION DE DONNÉES PAR SECTEUR



Source : IBM[9]

En 2022, une moyenne de 1,94 compromission d'au moins 500 dossiers médicaux a été signalée chaque jour.

Entre 2009 et 2022, **5 150 compromissions d'au moins 500 dossiers médicaux** ont été signalées.

Le nombre de compromissions d'au moins 500 dossiers médicaux signalées a **doublé au cours des 5 dernières années** (2018-2023).

Source : The HIPAA Journal[10]

Dans la mesure où tous les outils et technologies s'intègrent et fonctionnent en toute transparence avec l'architecture ouverte de ThreatQ, il n'est pas nécessaire de modifier l'infrastructure ou les workflows de sécurité existants. L'automatisation élimine les tâches répétitives et chronophages, permettant ainsi aux analystes de se concentrer sur des opérations prioritaires et stratégiques. La plate-forme permet en outre de partager rapidement des données de Threat Intelligence organisées, des conseils et des rapports avec un large éventail de parties prenantes internes et externes, y compris dans le secteur de la santé.

PRINCIPAUX ATOUTS DE THREATQ :

• **CONSOLIDATION** au sein d'un référentiel central de toutes les sources de données de Threat Intelligence et sur les vulnérabilités, tant les sources externes (p. ex. NH-ISAC) qu'internes (p. ex. SIEM)

• **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques

• **PRIORISATION** des mesures et ressources primordiales pour l'environnement du système de santé

• **INTÉGRATION** des indicateurs pertinents uniquement dans les stratégies de sécurité liées à la loi HIPAA

• **TRAQUE PROACTIVE** des activités malveillantes susceptibles de porter gravement atteinte aux dossiers des patients et aux établissements de santé

• **PRIORISATION** des vulnérabilités de sécurité connues et exploitées de manière active, risquant d'affecter la conformité réglementaire

• **ANALYSE ACCÉLÉRÉE** permettant de contrer plus rapidement les attaques visant plusieurs cibles, y compris les dispositifs médicaux connectés au réseau

• **DIFFUSION AUTOMATIQUE** des données de Threat Intelligence vers les outils de détection et de réponse à incident

Rendez-vous sur www.threatq.com/demo pour demander une démonstration en direct de la plate-forme ThreatQ et de ThreatQ TDR Orchestrator.

1. https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
2. https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html
3. https://www.chiefhealthcareexecutive.com/view/after-a-lull-ransomware-attacks-on-hospitals-are-rising-again
4. https://www.healthcareitnews.com/news/ransomware-attacks-have-doubled-2-years-report-shows
5. https://www.chiefhealthcareexecutive.com/view/after-a-lull-ransomware-attacks-on-hospitals-are-rising-again
6. https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
7. https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=393f4dcd6c88
8. https://www.hipaajournal.com/healthcare-data-breach-statistics/
9. https://www.ibm.com/downloads/cas/3R8N1DZJ
10. https://www.hipaajournal.com/healthcare-data-breach-statistics/

À PROPOS DE THREATQUOTIENT™

ThreatQuotient améliore les opérations de sécurité en regroupant des sources de données, des outils et des équipes hétérogènes afin d'accélérer la détection des menaces et la réponse à incident. La plate-forme d'opérations de sécurité orientée sur les données de ThreatQuotient permet aux équipes de prioriser les menaces, d'automatiser les tâches et de collaborer pour résoudre les incidents de sécurité. Elle permet une prise de décision plus ciblée et optimise les ressources limitées en intégrant les processus et technologies existants dans un espace de travail unifié. Résultat : une réduction des informations parasites, des menaces prioritaires claires et la possibilité d'automatiser les processus avec des données extrêmement fiables.

Les fonctionnalités de pointe en matière de gestion, orchestration et automatisation des données de ThreatQuotient prennent en charge de nombreux scénarios d'utilisation, notamment la réponse à incident, le Threat Hunting, la lutte contre le spear phishing, le tri des alertes et la priorisation des vulnérabilités. Par ailleurs, elles peuvent également servir de plate-forme de Threat Intelligence. ThreatQuotient est basé dans le nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe, en Asie-Pacifique et dans la région Moyen-Orient/Afrique du Nord. Pour plus d'informations, consultez le site www.threatquotient.com.

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147, États-Unis • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885

TQ-IDB06-1023-02